COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

10 Park Plaza – Suite 5170, Boston MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

DANIEL O'CONNELL
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

DANIEL C. CRANE
UNDERSECRETARY

Contact:
Rachael Liebert
(617)-973-8767
(857)-207-1550

CONSUMER ADVISORY
Protect Your Identity

In response to Countrywide's disclosure that 45,283 Massachusetts residents may have had their personal information compromised by a recent data breach, the Office of Consumer Affairs reminds consumers of the following steps they can take to protect their personal information.

What is identity theft?

Identity theft occurs when someone uses your personal identifying information, like your name, Social Security number, credit card number, or other financial information—without your permission to commit fraud or other crimes. Any time that a security breach occurs, whether through a large scale electronic data transmission or a small scale mishandling of paper records, consumers face an increased risk of identity theft.

Daniel Crane, Undersecretary of the Office of Consumer Affairs & Business Regulation, said, "Identity theft—a crime that affects millions of consumers—is escalating. It is important that Massachusetts consumers know how to reduce their chances of being victimized, and how to minimize the damage if their personal information is put at risk to be misused."

What should you do to prevent identity theft?

Never provide your personal information in response to an unsolicited request. Be wary of any contact from organizations that ask for personal information. Always ask for contact information to ensure the caller or sender is reputable.

Review your account statements regularly. By reviewing statements or viewing your bank account online, you could detect a theft and minimize its damage. If you suspect a security breach, contact the companies you do business with immediately.

Check your credit report regularly for accuracy and signs of fraudulent activity. Consumers are entitled to one free credit report every 12 months from each of the three national consumer reporting companies—Experian, Equifax, and TransUnion. You can receive a free credit report by phone, mail, or by visiting https://www.annualcreditreport.com.

Do not use personal information for passwords. Be sure your passwords contain at least eight characters and include numbers or symbols. Do not write down passwords or PINs (personal identification numbers).

Update your computer's anti-virus and firewall software regularly. If your anti-virus software does not have built-in spyware detection, invest in a spyware scanner as well as an anti-virus package and run scans at least once a week.

What should you do if you believe that your personal information may have been exposed to misuse?

If you believe that your personal information has been exposed to misuse:

1. *Place a fraud alert on your credit report. Call one of the major credit reporting agencies listed below:*

Equifax: Call (800) 525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241.

Experian: Call (888) 397-3742, and write: P.O. Box 9532, Allen, TX 75013.

TransUnion: Call (800) 680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790 Fullerton, CA 92834-6790.

The credit bureau you call is required by law to contact the other two. The fraud alert will remain in your credit file for at least 90 days. It requires creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts.

2. *Order a copy of your credit report and check it for unauthorized activity.*

If you notice questionable activity in your credit report, you can extend the fraud alert on your credit report. You must file a police report with your local police department, keep a copy for yourself, and provide a copy to one of the major credit bureaus. The extended fraud alert will be placed on your credit file for seven years.

3. *Monitor your financial accounts for suspicious activity.*

Check your bank accounts and credit card statements regularly for any unexplained activity or unauthorized transactions. If you notice unexplained activity, contact the fraud department of your financial institution and dispute any unauthorized transactions. Close accounts that have been tampered with or opened fraudulently.

What additional steps should you take if you believe that your personal information has been stolen or misused?

Place a Security Freeze on your Credit Reports

Under the new identity theft protection law that Governor Patrick signed in August 2007, Massachusetts consumers can place a security freeze on their credit reports.

A security freeze prohibits, with certain specific exceptions, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.

To place a security freeze on your credit report, you must send a written request to all three credit reporting agencies listed below.

Equifax Security Freeze
Experian Security Freeze
TransUnion Security Freeze

Within three business days after receiving your letter, the credit reporting agencies will place a freeze on providing credit reports to potential creditors.

If you are a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, temporarily lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee of up to $5 to place, lift, or remove a security freeze.

For more information about identity theft, call the Office of Consumer Affairs and Business Regulation Consumer Hotline at (617) 973-8787 or toll free (in Massachusetts) at (888) 283-2757. Or, visit our web site at www.mass.gov/consumer.